



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/994,476

11/26/2001

Ari Juels

1048-016

7236

80360 7590 11/26/2008
Bainwood, Huang & Associates, LLC
2 Connector Road
Westborough, MA 01581

EXAMINER

WILLIAMS, JEFFERY L

ART UNIT

PAPER NUMBER

2437

MAIL DATE

DELIVERY MODE

11/26/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 09/994,476	Applicant(s) JUELS ET AL.	
	Examiner JEFFERY WILLIAMS	Art Unit 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 September 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1, 2, 4 – 28, 38, 40 – 45 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, 2, 4 – 28, 38, 40 – 45 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response to the communication filed on 9/8/08.
All objections and rejections not set forth below have been withdrawn.
Claims 1, 2, 4 – 28, 38, 40 – 45 are pending.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/8/08 has been entered.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 16 – 28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1

2 Claim 16 provides for the use of “a decodable design comprising...”, but, since
3 the claim does not set forth any steps involved in the method/process, it is unclear what
4 method/process applicant is intending to encompass. A claim is indefinite where it
5 merely recites a use without any active, positive steps delimiting how this use is actually
6 practiced.

7 Regarding claim 17, the recitation, “selecting a subset of the coordinate sets in
8 the first sequence such that the first value in each subset coordinate set corresponds to
9 the first value of at least one coordinate set in the first sequence” is essentially unclear
10 as it appears that the applicant is merely reciting the nature of a subset (i.e. that a value
11 within a subset of the first sequence will correspond to a value within the first
12 sequence).

13 Claim 17 recites the limitations “the coordinate sets” in line 6 and “the first value
14 in each subset coordinate set” in line 7. There is insufficient antecedent basis for these
15 limitations in the claim. For the purpose of examination, the examiner presumes claim
16 17 to recite “coordinate sets” and “a first value in a subset coordinate set”.

17 Claim 17 recites “applying an error-correcting function *to the subset*” and
18 “outputting *the subset*.” These recitations are unclear as the applicant previously recites
19 both a “subset of the coordinate sets” and “each subset coordinate set”, and the
20 applicant has failed to clearly identify the claimed “subset”.

21 Claim 18 recites the limitations “the error correcting code c” in line 8. This
22 recitation lacks antecedent basis and is unclear. Applicant has previously recited

1 "codeword c". For the purpose of examination, the examiner presumes claim 18 to
2 recite "the error-correcting code".

3 Claim 18 recites the limitations "outputting the second codeword c' ". There is
4 insufficient antecedent basis for these limitations in the claim. For the purpose of
5 examination, the examiner presumes claim 18 to recite "outputting the second
6 codeword (c' d(B, E))", in harmony with prior recitations.

7 Claim 19 is rejected under 35 U.S.C. 112, second paragraph, as being
8 incomplete for omitting essential steps, such omission amounting to a gap between the
9 steps. See MPEP § 2172.01. The omitted steps involve the creation of the "order-
10 invariant fuzzy commitment". The examiner notes that the missing steps must occur
11 before an "order-invariant fuzzy commitment" can be stored.

12 Claim 24 provides for the use of "a Reed-Solomon error detecting code", but,
13 since the claim does not set forth any steps involved in the method/process, it is unclear
14 what method/process applicant is intending to encompass. A claim is indefinite where it
15 merely recites a use without any active, positive steps delimiting how this use is actually
16 practiced.

17 Any claims depending upon the above rejected claims are rejected by virtue of
18 dependency.

19

20

21

22

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1, 2, 4 – 28, 38, 40 – 45 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding claims 1, 2, 4 – 28, 38, 40 – 45, they are directed to recitations of an abstract idea, such as the creation of a data sequence or the manipulation of a data sequence. However, the claims fail to recite a final result achieved by the invention that is useful, tangible, and concrete. The examiner notes that claims directed towards generation of a set of numbers or the conversion of set of numbers does not manipulate appropriate subject matter and thus does not constitute a statutory process.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1 **Claims 17, 19 – 28, and 38 are rejected under 35 U.S.C. 102(b) as being**
2 **anticipated by Juels et al. (Juels), “A Fuzzy Commitment Scheme”.**

3
4
5
6 Regarding claim 17, Juels discloses:

7 *receiving a first input element including a sequence of one or more values from a*
8 *predetermined set (pg. 32-33, “example 2”, par. 3, x’);*

9 *receiving an order-invariant fuzzy commitment sequence (pg. 32-33, “example*
10 *2”, par. 1 ,2);*

11 *constructing a set of integers having a predetermined number of elements*
12 *representing respectively values in the first input element (pg. 32-33, “example 2”, par.*
13 *2);*

14 *selecting a subset of the coordinate sets in the first sequence such that the first*
15 *value in each subset coordinate set corresponds to the first value of at least one*
16 *coordinate set in the first sequence; applying an error-correcting function to the subset;*
17 *and outputting the subset (pg. 32-33, “example 2”, par. 3).*

18
19 Regarding claim 19, Juels discloses:

20 *receiving a first set of elements; and selecting a polynomial for encoding the item*
21 *under the first set of elements to generate an order-invariant fuzzy commitment of the*
22 *item (pg. 30, col. 2, par. 3, 4); and storing said commitment in a computing device (pg.*
23 *31, col. 2, par. 5).*

24

1 Regarding claim 20, Juels discloses:

2 *further including inserting chaff points that form a part of the commitment of the*
3 *item* (pg. 31, section 3.1, par. 3, section 4.1, par. 2; pg. 32, col 1, par. 1,2).

4
5 Regarding claim 21, Juels discloses:

6 *further including receiving a second set of elements; and selectively*
7 *decommitting the item based upon a level of overlap of the first and second sets of*
8 *elements* (pg. 32, col. 1, par. 3, 4).

9
10 Regarding claims 22 – 28, Juels discloses:

11 *further including determining the polynomial from the second set of elements if*
12 *the level of overlap is greater than a predetermined threshold; further including utilizing*
13 *an error-correcting code for determining the polynomial; utilizing a decodable design to*
14 *decommit the item, wherein the decodable design includes constituent pairs of sets*
15 *having a level of overlap less than a predetermined level* (pg. 32, col. 1, par. 3); *utilizing*
16 *a Reed-Solomon error detecting code* (pg. 34, col. 2); *wherein the first set of elements*
17 *corresponds to a biometric template* (pg. 29, section 2.1); *hiding the first set of*
18 *elements in a target set containing a plurality of elements selected from a field; further*
19 *including projecting the first set of elements onto the target set* (pg. 30 – 31, section 3).

20
21 Regarding claim 38, it is a program claim essentially corresponding to the
22 method of claims 19 - 28, and it is rejected, at least, for the same reasons.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

Response to Arguments

Applicant's arguments filed 9/8/08 have been fully considered but they are not persuasive.

Applicant asserts essentially that:

(i) *If the rejection of claim 38 as amended is to be maintained, Applicants respectfully request that it be pointed out with particularity where the cited prior art teaches an article comprising a machine readable medium that stores executable code instructions for enabling the step of "receiving the order-invariant fuzzy commitment" as claimed by the Applicants (Remarks, pg. 15, par. 3)*

In response, the examiner respectfully notes that the prior art discloses a computer system, and thus means for executing the computer system's functions (i.e. a machine readable medium that stores executable code instructions") for enabling the step of "receiving the order-invariant fuzzy commitment" (Juels, Abstract; sect. 2.1)

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

See Notice of References Cited.

A shortened statutory period for reply is set to expire **3** months (not less than 90 days) from the mailing date of this communication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Art Unit: 2437

1 Information regarding the status of an application may be obtained from the
2 Patent Application Information Retrieval (PAIR) system. Status information for
3 published applications may be obtained from either Private PAIR or Public PAIR.
4 Status information for unpublished applications is available through Private PAIR only.
5 For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should
6 you have questions on access to the Private PAIR system, contact the Electronic
7 Business Center (EBC) at 866-217-9197 (toll-free).

8
9
10 J. Williams
11 AU 2437
12
13 /Emmanuel L. Moise/
14 Supervisory Patent Examiner, Art Unit 2437
15